Roboter und Privacy: Informationsrechtliche Herausforderungen datenbasierter Systeme

Früh, Alfred

Roboter und Privacy

Informationsrechtliche Herausforderungen datenbasierter Systeme

Alfred Früh*

Roboter – hier verstanden als datenbasierte Systeme – können in den unterschiedlichsten Bereichen eingesetzt werden. Gemeinsam ist ihnen, dass sie mittels Sensoren in komplexen Umweltsituationen Daten aufnehmen, selbständig Programmabläufe anpassen und damit zunehmend autonom handeln. Aus informationsrechtlicher Sicht stellen diese datenbasierten Systeme die Rechtsordnung vor erhebliche Probleme. Insbesondere das Datenschutzrecht reicht gleichzeitig zu weit und zu wenig weit; es besteht eine grundlegende Diskrepanz zwischen dessen Schutzwirkungen und dessen Schutzgegenstand. In der Wissenschaft wird gegenwärtig zwei Lösungsansätzen zugetraut, diese strukturellen Probleme zu lösen: dem Dateneigentum und einer Neukonzeption des Schutzgegenstands «Privacy». Der Beitrag stellt diese beiden Ansätze vor und beleuchtet die in sie gesetzten Erwartungen sowie mögliche Schwierigkeiten.

Les robots, qui désignent ici des systèmes basés sur des données, peuvent être utilisés dans les domaines les plus variés. Ils ont en commun d'enregistrer des données dans des environnements complexes grâce à des capteurs, d'adapter eux-mêmes les déroulements de programme et d'agir ainsi de manière toujours plus autonome. Du point de vue du droit de l'information, ces systèmes basés sur des données posent d'importants problèmes à l'ordre juridique. En particulier, le droit de la protection des données va trop loin tout en étant insuffisant ; il y a un profond écart entre ses effets de protection et l'objet même de sa protection. La science se fie actuellement à deux approches susceptibles de résoudre ces problèmes structurels : la propriété des données et une nouvelle appréhension conceptuelle du bien protégé que constitue la « privacy ». L'article présente les deux approches et met en évidence les attentes qu'elles suscitent ainsi que les éventuelles difficultés.

Inhaltsübersicht

I. Einleitung

Dies ist kein Beitrag über Roboter als Objekte oder Subjekte des Rechts. Abwegig wäre dies zwar nicht; die Diskussion um die rechtliche Erfassung künstlicher Intelligenz hat längst begonnen und Erörterungen über moralisches Handeln von Maschinen schaffen es regelmässig bis in die Tagespresse. Drängender als die Statusdebatten um den Roboter[1] scheint aber gegenwärtig (noch) die Frage, vor welche Herausforderungen Roboter die Gesellschaft aus informationsrechtlicher Sicht stellen.

Als Roboter muss man dabei aber nicht mehr nur eine Maschine verstehen, die abhängig von menschlicher Anweisung mechanische Bewegungen ausführt. Vielmehr geht es mittlerweile um Maschinen, die mittels Sensoren in komplexen Umweltsituationen Daten aufnehmen, selbständig Programmabläufe anpassen und verbessern können und damit zunehmend autonom handeln.[2] Bei der Untersuchung solcher datenbasierten Systeme kann aus informationsrechtlicher Sicht auf Forschung in zwei Bereichen zurückgegriffen werden: Einerseits hat sich die Rechtswissenschaft bereits mit dem Internet der Dinge

* Alfred Früh, Dr. iur., Rechtsanwalt, Postdoktorand und Geschäftsführer des Center for Information Technology, Society, and Law (ITSL) an der Universität Zürich.

1 Siehe hierzu Susanne Beck, Über Sinn und Unsinn von Statusfragen – zu Vor- und Nachteilen der Einführung einer elektronischen Person, in: Eric Hilgendorf/Jan-Philipp Günther (Hrsg.), Robotik und Gesetzgebung, Baden-Baden 2013, 239 ff.; vgl. Susanne Beck, Der rechtliche Status autonomer Maschinen, AJP 2017, 183 ff.

2 Gerald Spindler, Zivilrechtliche Fragen beim Einsatz von Robotern, in: Eric Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, Baden-Baden 2014, 63 ff., 63; s.a. Eric Hilgendorf, Vorwort, in: Eric Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, Baden-Baden 2013, 5, m.H. auf die Disziplin der Autonomik; vgl. Isabelle Wildhaber/Melinda Lohmann, Roboterrecht – eine Einleitung, AJP 2017, 135 ff.

bzw. IoT *(internet of things)* befasst,[3] welches sich unter anderem dadurch auszeichnet, dass physische Objekte massenhaft Sensordaten erheben. Andererseits werden seit längerem die rechtlichen Implikationen von Big Data, das heisst der Erhebung und Analyse von grossen, ungeordneten Datenmengen, untersucht.[4]

Privacy[5] spielt im Bereich datenbasierter Systeme insoweit eine Rolle, als Menschen durch bestimmte (Nutzungs-)Handlungen die Datenerhebung auslösen, steuern oder beeinflussen oder selbst Gegenstand der Datenerhebung sind. Aus informationsrechtlicher Sicht ist dies relevant, weil diese Menschen Grundrechtsträger (namentlich des Rechts auf Privatsphäre, Art. 13 BV, insbes. Abs. 2) sind, Persönlichkeitsrechte haben (Art. 28 ff. ZGB) und als betroffene Personen im Sinne des Datenschutzgesetzes (DSG) gelten. Aus den stetig zunehmenden Datenströmen lassen sich wertvolle Informationen gewinnen, die (nicht nur, aber auch) Aussagen über diese Menschen ermöglichen.

Aus informationsrechtlicher (insbesondere datenschutzrechtlicher) Sicht stellen diese Entwicklungen die Rechtsordnung vor erhebliche Probleme. Nachfolgend wird der Versuch unternommen, diese Probleme zu erfassen (II.), bevor dann die aktuell diskutierten Lösungsansätze erörtert werden (III.). Der Beitrag schliesst mit einem kurzen Fazit (IV.).

II. Problemstellung

Das Datenschutzrecht wird aufgrund seines weiten Anwendungsbereichs, seines präventiven Charakters und der strengen Grundsätze der Datenbearbeitung zunehmend zu einer erheblichen Hürde für unternehmerische und wissenschaftliche Tätigkeit (sogleich II.A.). Gleichzeitig zeigt sich trotz des weiten Anwendungsbereichs, dass die Interessen der betroffenen Personen, insbesondere deren Privacy, oft nicht oder nicht ausreichend geschützt sind (unten II.B.).

A. Zu weit reichender Datenschutz

In jüngerer Vergangenheit wird vermehrt darauf hingewiesen, dass die Einhaltung datenschutzrechtlicher Bestimmungen die Unternehmen vor grosse Schwierigkeiten stellt.[6] Dies gilt im Grundsatz für sämtliche von der Digitalisierung betroffenen Branchen – und damit praktisch für alle Unternehmen. Ins Feld geführt wird, dass die Datenschutz-Compliance bei den Unternehmen unverhältnismässige Kosten verursache oder bestimmte Geschäftsmodelle unterbinde und der Datenschutz so letztlich zur Innovationsbremse werde.[7] Dass der Datenschutz aus Sicht der Unternehmen einen unerwünschten Kostenfaktor darstellt und als zu weit reichend eingeschätzt wird, erstaunt kaum. Bemerkenswert ist aber, dass der Datenschutz auch den Allgemeininteressen zuwiderlaufen kann. Ein grosser Datenfundus erlaubt in vielerlei Hinsicht Anwendungen, die sowohl dem Einzelnen als auch der Gesellschaft Nutzen stiften können. Im Bereich der Gesundheitsdaten wird dies ohne weiteres deutlich: Je grösser die ihnen zugrunde liegenden Datenbestände sind, desto präziser können Diagnosen oder Behandlungsentscheidungen sein. Dass in der medizinischen Forschung die Erhebung und Verwendung gesundheitsrelevanter Daten durch datenschutzrechtliche Hürden vereitelt zu werden drohen, muss deswegen kritisch gesehen werden.[8] Zudem sind Daten – auch personenbezogene Daten – eine wichtige Ressource, mithin das Fluidum unseres Zusammenlebens.[9] Auf dieser Basis kann festgehalten werden, dass eine extensive Anwendung datenschutzrechtlicher Bestimmungen in einen Konflikt mit Freiheitsrechten wie der Wirtschaftsfreiheit, der Wissenschaftsfreiheit und der Informationsfreiheit geraten kann.[10]

Belastbare *empirische* Grundlagen zu diesen Effekten des Datenschutzes auf Wirtschaft und Wissenschaft schei-

---

3 Siehe z.B. Florian Sprenger/Christoph Engemann (Hrsg.), Internet der Dinge, Bielefeld 2015; Rolf H. Weber/Romana Weber, Internet of Things, Zürich 2010.

4 Siehe Viktor Mayer-Schönberger/Kenneth Cukier, Big Data, A Revolution, New York 2013; Astrid Epiney/Daniela Nüesch (Hrsg.), Big Data und Datenschutzrecht, Zürich 2016; Rolf H. Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014; sowie digma 1/2013 und Jusletter IT vom 21.5.2015.

5 In der hier verwendeten Form geht der Begriff «Privacy» über den Begriff «Privatsphäre» hinaus; es klingt auch das Instrument des *privacy law* (d.h. des Datenschutzrechts) an, welches diese Privatheit vorrangig garantieren soll.

6 Im Zusammenhang mit Big Data: Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning?, 3 International Data Privacy Law 2013, 1 ff.; Rolf H. Weber/Florent Thouvenin, Einleitung, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 1 f.

7 Nikolai Horn, Law by Code – den digitalen Wandel regeln, FAZ vom 14.9.2016; ähnlich pointiert Niko Härting, Internetrecht, 5. A., Köln 2014, 627; vorsichtiger Daniel Rücker, Datenschutz, in: Peter Bräutigam/Thomas Klindt (Hrsg.), Digitalisierte Wirtschaft/Industrie 4.0, München 2015, 30 ff., 38.

8 Aus diesem Grund enthält Art. 32 des Humanforschungsgesetzes (HFG; SR 810.30) die Möglichkeit eines Generalkonsents, was allerdings noch nicht alle Probleme löst; siehe dazu auch SAMW Bulletin 3/2016.

9 Thomas Giesen, Demokratiewidrig, Süddeutsche Zeitung vom 18.5.2012, 12; s.a. Härting (FN 7), 630, m.H. auf Wikipedia.

10 Härting (FN 7), 627.

nen gegenwärtig noch zu fehlen.[11] Dies dürfte sich aber bald ändern. Insbesondere werden künftig wohl mehr Daten über die Kosten unternehmerischer Datenschutz-Compliance erhältlich sein, weil die Missachtung der Datenschutzbestimmungen für die Unternehmen gravierende Folgen haben kann. Die auf europäischer Ebene kürzlich erlassene Datenschutz-Grundverordnung (EU-DSGVO)[12] sieht in ihrem Art. 83 neu Geldbussen für Datenschutzverstösse vor, und allgemein wird erwartet, dass sich das im Revisionsprozess befindliche Schweizer DSG ebenfalls an dieser Vorgabe orientieren wird.

Es deutet einiges darauf hin, dass der Datenschutz in seinem Anwendungs- und Wirkungsbereich heute zu weit reicht. *Konkret* lässt sich dies wie folgt aufzeigen: in formeller Hinsicht durch die Ausweitung des Anwendungsbereichs (II.A.1.), in konzeptioneller Hinsicht am präventiven Ansatz des Datenschutzrechts (II.A.2.) und schliesslich auch in materieller Hinsicht bei den Grundsätzen der Datenbearbeitung (II.A.3.).

1. Formell: Anwendungsbereich

a. Weiter Begriff der Datenbearbeitung

Das Datenschutzgesetz verlangt die Rechtmässigkeit der Datenbearbeitung (Art. 4 Abs. 1 DSG). Gemäss Art. 3 lit. e DSG wird unter Datenbearbeitung jeder Umgang mit Personendaten unabhängig von den angewandten Mitteln und Verfahren verstanden. Umfasst ist insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten. Damit ist also letztlich alles, was man mit Personendaten tut, ein solcher «Umgang».[13] In Bezug auf datenbasierte Systeme liegt nach vorherrschender Rechtsauffassung auch dann eine Bearbeitung vor, wenn das System Daten sammelt, welche dieses System nie verlassen oder die nur mit erheblichem Aufwand auszulesen sind.[14]

Der Begriff der Datenbearbeitung wird technikneutral verstanden. Erfasst ist deswegen sowohl die manuelle als auch die automatische Bearbeitung von Personendaten. Ein Gespräch über einen abwesenden Arbeitskollegen ist genauso eine Datenbearbeitung wie die automatisierte Gesichtserkennung mit einer «Datenbrille». Auf diese Weise dehnt sich der Anwendungsbereich des Datenschutzrechts durch neue technische Entwicklungen tendenziell aus. Das gilt insbesondere für datenbasierte Systeme. Allerdings bedeuten weder das Aufkommen datenbasierter Systeme noch die Digitalisierung selbst für das Datenschutzrecht einen Paradigmenwechsel:[15] Bereits vor mehr als 35 Jahren – und damit in der Prä-Internet-Ära – wurde festgestellt, dass die Möglichkeiten der automatischen Datenverarbeitung zu ganz neuen Herausforderungen führen.[16]

Zu einem gewissen Grad neu ist freilich, dass sich digitale Datenbearbeitungen – anders als noch in der analogen Welt – potenziell ubiquitär und ohne zeitliche Begrenzung auswirken können. Eine einmal digital erhobene Information über eine Person kann sehr einfach zu einem späteren Zeitpunkt in einem ganz anderen Kontext relevant werden. Beispielsweise könnten auch noch Jahre später Kundeninformationen eines Carsharing-Betreibers mit den durch den Fahrzeughersteller gesammelten Bewegungsprofilen gewisser Fahrzeuge kombiniert werden, um Kenntnisse über den Aufenthalt einer Person zu einem bestimmten Zeitpunkt zu erlangen.[17] Auch dies bewirkt in gewissem Sinn eine Ausdehnung des Anwendungsbereichs, wenn auch nicht in sachlicher, sondern in zeitlicher und räumlicher Hinsicht.

b. Personenbezogenheit der Daten

Das DSG definiert den Begriff der Personendaten in Art. 3 lit. a DSG. Personendaten sind demnach alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Eine Person ist dann bestimmt, wenn sie zweifelsfrei identifizierbar ist. Sie ist dann bestimmbar, wenn die je-

---

11 Zum Kontext Big Data siehe Rolf H. Weber, Big Data: Sprengkörper des Datenschutzrechts, Jusletter IT vom 11.12.2013, N 5.

12 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119, 4.5.2016, 1–88.

13 Beat Rudin, Art. 3 N 32, in: Bruno Baeriswyl/Kurt Pärli (Hrsg.), Datenschutzgesetz (DSG), Bern 2015 (zit. SHK DSG-Verfasser).

14 Im Rahmen des Deutschen Datenschutzgesetzes werden hierzu einige Differenzierungen angestellt, siehe Berthold H. Haustein, Herausforderungen des Datenschutzrechtes vor dem Hintergrund aktueller Entwicklungen in der Robotik, in: Eric Hilgendorf/Jan-Philipp Günther (Hrsg.), Robotik und Gesetzgebung, Baden-Baden 2013, 91 ff., 97.

15 In Bezug auf die Robotik: Haustein (FN 14), 100: «Die moderne Robotik basiert unter anderem auf der Erhebung, Übertragung und Verarbeitung grosser Datenmengen. Insofern besteht im Zusammenhang mit dem Datenschutzrecht nur eine quantitative Neuerung, keine qualitative.»

16 Michael Bogdan, «Dataflykt over gränserna och den svenska datalagstiftningen», 1 Svensk Juristtidning 1978, übersetzt in: Christopher Kuner/Fred H. Cate/Christopher Millard/Dan Jerker B. Svantesson, The (Data Privacy) Law Hasn't even Checked in when Technology Takes off, 4 International Data Privacy Law 2014, 175.

17 Ob diese Tatsache ein «Recht auf Vergessenwerden» begründen kann, ist eine andere Frage, die hier nicht erörtert werden kann; kritisch hierzu Härting (FN 7), 623.

weilige Information allein zwar keinen eindeutigen Rückschluss auf die Identität zulässt, die Identifikation aber dennoch aufgrund der vorhandenen Informationen möglich ist. Der Personenbezug muss sich ohne unverhältnismässigen Aufwand erstellen lassen und es muss damit gerechnet werden, dass dieser potentiell erfolgt.[18] Angesichts der heutigen informationstechnischen Möglichkeiten ist der für die Bestimmung von Personen notwendige Aufwand praktisch nie mehr unverhältnismässig.[19]

Anders mag es *prima vista* aussehen, wenn besondere Techniken angewendet werden, um den Personenbezug der Daten zu entfernen. Beim Verfahren der *Pseudonymisierung* wird die Verknüpfbarkeit eines Datenbestandes mit der wahren Identität der betroffenen Person verringert.[20] Typischerweise wird ein Merkmal eines Datensatzes durch ein anderes ersetzt.[21] Von einer *Anonymisierung* spricht man demgegenüber nur dann, wenn eine Identifizierung unwiderruflich unmöglich gemacht wird.[22]

Gerade dies lässt sich aber nicht garantieren. Im Zeitalter der Big Data-Anwendungen können auch (scheinbar) anonymisierte Daten wieder re-individualisiert (oder re-personalisiert) werden,[23] was hinreichend durch Studien belegt wurde.[24] Die Re-Individualisierung einer Person ist umso wahrscheinlicher, je mehr Daten vorhanden sind.[25] Dies heisst zwar nicht, dass eine Anonymisierung *per se* ausgeschlossen ist, aber eine Anonymisierung «ein für alle Mal» gibt es nicht mehr.

Stattdessen muss Anonymisierung in Bezug auf die verfolgten Zielsetzungen sorgfältig geplant werden. Die gewählten Anonymisierungstechniken[26] müssen kontextabhängig gewählt und letztlich auch kontinuierlich überprüft werden.[27] Solange dies nicht geschieht, muss in sehr vielen Bereichen – insbesondere im Zusammenhang mit datenbasierten Systemen[28] – davon ausgegangen werden, dass es sich um personenbezogene Daten handelt und der Anwendungsbereich des Datenschutzgesetzes erstellt ist. Das DSG ist aber nicht auf Situationen ausgelegt, in denen Daten zu einem späteren Zeitpunkt aufgrund möglicher Re-Individualisierung «plötzlich» dem Datenschutzrecht unterstellt sind. Die Lehre will – soweit sie sich mit dieser Frage befasst – die datenschutzrechtlichen Grundsätze auch *ex post* voll auf re-individualisierte Daten anwenden.[29] Für die Zeit, in der die Daten (vermeintlich) anonymisiert waren, werden Datenbearbeitungen zwar nicht rückwirkend rechtswidrig.[30] Dennoch ist es für den Datenbearbeiter sehr schwierig, nach der Re-Individualisierung erfolgte Datenbearbeitungen (insbesondere durch Einwilligung) zu rechtfertigen. Zudem kann die betroffene Person ihre Informations- und Auskunftsansprüche typischerweise nicht durchsetzen.[31]

Mit der Zunahme der Fälle, in denen Daten (trotz Vorkehrungen zur Anonymisierung) einen Personenbezug

---

18 Rolf H. Weber/Dominic Oertly, Aushöhlung des Datenschutzes durch De-Anonymisierung bei Big Data Analytics?, Jusletter IT vom 21.5.2015, N 6.

19 Bruno Baeriswyl, Big Data zwischen Anonymisierung und Re-Individualisierung, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Zürich 2014, 45 ff., 50; Rolf H. Weber, Big Data: Herausforderungen für das Datenschutzrecht, in: Astrid Epiney/Daniela Nüesch (Hrsg.), Big Data und Datenschutzrecht, Zürich 2016, 6; von der gleichen Grundannahme geht die SAMW für die von ihr entwickelte Vorlage eines Generalkonsents aus, SAMW Bulletin 3/2016, 3.

20 Artikel-29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken, 10.4.2014, 3 f., Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf (Abruf 11.1.2017).

21 Artikel-29-Datenschutzgruppe (FN 20), 24.

22 Artikel-29-Datenschutzgruppe (FN 20), 3. Dies bedeutet im Grunde auch, dass der bisweilen verwendete Begriff De-Anonymisierung nicht verwendet werden sollte; siehe hierzu auch Weber/Oertly (FN 18), N 14.

23 Michael Dorner, Big Data und «Dateneigentum», CR 2014, 617 ff., 628; Roland Mathys, Was bedeutet Big Data für die Qualifikation als besonders schützenswerte Personendaten?, Jusletter IT vom 21.5.2015, N 2 und 5; Thomas Heymann, Rechte an Daten, CR 2016, 650 ff., 656.

24 Melissa Gymrek et al., Identifying Personal Genomes by Surname Inference, 339 Science 2013, 321 ff.; siehe weiter die Untersuchung von Latanya Sweeney, Simple Demographics Often Identify People Uniquely, Data Privacy Working Paper, 2000, mit öffentlich verfügbaren Daten, Internet: http://dataprivacylab.org/projects/identifiability/paper1.pdf (Abruf 4.12.2016), und eine Studie von Philippe Golle, Revisiting the Uniqueness of Simple Demographics in the US Population, Proc. 5th ACM Workshop on Privacy in Electronic Society, 2006, basierend auf jüngeren Daten, Internet: https://crypto.stanford.edu/~pgolle/papers/census.pdf (Abruf 4.12.2016).

25 Weber (FN 11), N 12; Baeriswyl (FN 19), 52; Bruno Baeriswyl, «Big Data» ohne Datenschutz-Leitplanken, digma 2013, 14 ff., 15 (zit. Baeriswyl, digma).

26 Zu jenen Günther Karjoth, Sind anonymisierte Daten anonym genug? Von den (begrenzten) technischen Möglichkeiten, persönliche Daten in eine perfekte anonyme Form zu wandeln, digma 2008, 18 ff.; Kai Hofmann/Gerrit Hornung, Rechtliche Herausforderungen des Internets der Dinge, in: Florian Sprenger/Christoph Engemann (Hrsg.), Internet der Dinge, Bielefeld 2015, 181 ff., 195, Fn 53; Artikel-29-Datenschutzgruppe (FN 20), 13 f.

27 Artikel-29-Datenschutzgruppe (FN 20), 28 f.

28 Für vernetzte Fahrzeuge beispielsweise Rolf Schwartmann/Christian-Henner Hentsch, Parallelen aus dem Urheberrecht für ein neues Datenverwertungsrecht, PinG 2016, 117 ff., 121.

29 Astrid Epiney, Big Data und Datenschutzrecht: Gibt es einen gesetzgeberischen Handlungsbedarf?, Jusletter vom 21.5.2015, N 28.

30 Epiney (FN 29), N 29.

31 Baeriswyl, digma (FN 25), 15, spricht deswegen von einer datenschutzrechtlichen «Zeitbombe».

aufweisen, dehnt sich auch der Anwendungsbereich des Datenschutzrechts aus.[32] Auch die Rechtsprechung hat diese durch die technische Entwicklung angestossene Ausdehnung längst aufgenommen.[33] Konsequenterweise kommt man nicht umhin, vor diesem Hintergrund auch die Unterscheidung von personenbezogenen Daten und Sachdaten insgesamt in Frage zu stellen,[34] was das hier beschriebene Problem eines zu weit reichenden Datenschutzes freilich noch einmal verschärft.[35]

2. Konzeptionell: Präventiver Ansatz

Das DSG bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden (Art. 1 DSG). Schutzgegenstand ist damit die Persönlichkeit der betroffenen Personen. In Art. 12 DSG wird sodann ausgeführt, eine Datenbearbeitung dürfe nicht persönlichkeitsverletzend sein. Dies ist bereits dann der Fall, wenn die Grundsätze der Datenbearbeitung nicht eingehalten werden (Art. 12 Abs. 2 lit. a DSG). Die Verletzung eines datenschutzrechtlichen Grundsatzes, etwa das Nichteinhalten der Zweckbindung, stellt damit schon eine Persönlichkeitsverletzung dar.[36]

Daraus geht hervor, dass sich der Schutzgegenstand des Datenschutzrechts zwar am Persönlichkeitsrecht orientiert, aber *mindestens* so weit reicht wie die von jenem geschützte Privatsphäre.[37] Auf diese Weise ist eine gewisse Loslösung vom Schutzgegenstand Privacy bereits im DSG selbst angelegt. Datenbearbeitungen gelten also bereits dann als unzulässig, wenn eine bloss abstrakte Gefährdung der Persönlichkeit vorliegt. Im Zuge der Rechtsprechung haben sich zusätzliche Facetten des Schutzzwecks herausgebildet, die zum Teil ebenfalls über das herkömmliche Verständnis des Persönlichkeitsschutzes hinausgehen. Neben dem Recht auf informationelle Selbstbestimmung sind dies insbesondere Ansätze eines Rechts auf Vertraulichkeit und Integrität und neuerdings eines *«right to be forgotten»*.[38] Der Anspruch, die Persönlichkeit der betroffenen Person möglichst umfassend zu schützen, wurde aber gleichwohl beibehalten. Damit folgt das Datenschutzrecht mit Blick auf den Schutzgegenstand Privacy einem sehr präventiven Ansatz, der dafür sorgt, dass sehr viele Verhaltensweisen vom Anwendungsbereich umfasst sind.

3. Materiell: Grundsätze der Datenbearbeitung

Wie weit das Datenschutzrecht tatsächlich reicht, zeigt sich erst bei der Anwendung des materiellen Rechts. Die massenhafte Verwendung von Sensordaten bei datenbasierten Systemen führt zu grundsätzlichen Widersprüchen mit dem Datenschutzrecht.[39] Dies gilt jedenfalls dann, wenn Daten massenhaft gesammelt und dauerhaft gespeichert werden. Es spricht wenig dafür, dass dies bei datenbasierten Systemen wie z.B. selbstfahrenden Autos anders sein sollte. Auch jene fällen bessere Entscheidungen, je grösser die Datenbasis ist.[40]

Bei der Bearbeitung von Personendaten müssen die in Art. 4 DSG niedergelegten Grundsätze der Datenbearbeitung eingehalten werden. Im Einzelnen präsentiert sich die Lage wie folgt:

– Der *Grundsatz der Verhältnismässigkeit* (Art. 4 Abs. 2 DSG) kann bei der massenhaften Verwendung von Daten nicht eingehalten werden. Insbesondere der Grundsatz der Datenminimierung, der als Teilgehalt des Verhältnismässigkeitsprinzips verstanden wird, verträgt sich nicht mit der massenhaften Sammlung von Daten in datenbasierten Systemen. Härting bringt es wie folgt auf den Punkt: «Ein Stromzähler kann nur entweder ‹smart› oder ‹datensparsam› sein; nicht jedoch beides zugleich. Wer intelligente technische

---

[32] Auch innerhalb des Begriffs der Personendaten ist eine Ausweitung zu erkennen; selbst der Begriff der Gesundheitsdaten erfährt eine Ausdehnung, siehe Mathys (FN 23), N 13, mit Hinweisen auf die EU-DSGVO (FN 12) und die Arbeiten der Artikel-29-Datenschutzgruppe (FN 20).

[33] Zur (bejahten) Personenbezogenheit dynamischer IP-Adressen in der EU jüngst EuGH, Rs. C-582/14, 19.10.2016. Für dieselbe Frage in der Schweiz bereits BGE 136 II 508 E. 3 («Logistep»); s.a. die Vorinstanz in BVGer, A-3144/2008, 27.5.2009, E. 2.2.3.

[34] Dies klar ablehnend: Epiney (FN 29), N 30; ähnlich auch Schwartmann/Hentsch (FN 28), 120.

[35] Kritisch deswegen auch Weber (FN 11), N 24, und Baeriswyl (FN 19), 55.

[36] Vorbehalten bleibt selbstverständlich – wie auch bei Art. 28 ZGB – die Möglichkeit, diese Verletzung auf einer nachgelagerten Stufe zu rechtfertigen.

[37] Ebenso BSK DSG-Maurer-Lambrou/Kunz, Art. 1 N 13, in: Urs Maurer-Lambrou/Gabor-Paul Blechta (Hrsg.), Datenschutzgesetz (DSG), Öffentlichkeitsgesetz (BGÖ), Basler Kommentar, 3. A., Basel 2014. Zum Verhältnis von DSG und Privatsphäre siehe Stephan C. Brunner, Mit rostiger Flinte unterwegs in virtuellen Welten?, Jusletter vom 4.4.2011, N 3.

[38] Rolf H. Weber, Neue Grundrechtskonzeptionen zum Schutz der Privatheit, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich 2012, 7 ff.

[39] Alexander Rossnagel, Datenschutz in einem informatisierten Alltag, Berlin 2007, 205; Dorner (FN 23), 626; Nicolas P. Terry, Big Data Proxies and Health Privacy Exceptionalism, 24 Health Matrix: Journal of Law Medicine 2014, 65 ff.

[40] Härting (FN 7), 627.

Lösungen möchte, kann den Anbietern nicht zugleich Datenaskese verordnen.»[41]

– Der *Grundsatz der Zweckbindung* (Art. 4 Abs. 3 DSG) führt ebenfalls zu unüberwindbaren Hürden für datenbasierte Systeme. Er verlangt, dass Daten nicht für andere Zwecke verwendet werden, als bei der Beschaffung angegeben wurde. Der Zweck der Datenbearbeitung muss bereits im Voraus bekannt sein. Eine Datenbeschaffung «auf Vorrat» ist nicht zulässig. In datenbasierten Systemen wird mit der Datensammlung eine Grundlage für Entscheidungen geschaffen, obwohl diese Entscheidungen unter Umständen noch gar nicht antizipiert werden können.[42] Zumindest bei einer engen Interpretation dieses Grundsatzes müssten viele Big Data-Anwendungen an den Vorgaben des Datenschutzrechts scheitern.[43]
– Der *Grundsatz der Erkennbarkeit* (Art. 4 Abs. 4 DSG) sieht vor, dass die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung für die betroffenen Personen erkennbar sein muss. Dies ist aber bei von Sensoren erfassten Daten in der Regel nicht der Fall. Zwar steht das Erfordernis der Erkennbarkeit der Anwendung von datenbasierten Systemen nicht grundsätzlich entgegen, es erhöht aber die Anforderungen an deren Betrieb.[44]

B. Zu wenig weit reichender Datenschutz

Trotz seiner augenfälligen Reichweite scheint der Datenschutz nicht oder nur teilweise die Wirkungen zu entfalten, die man sich von ihm erhofft. Für den unzulänglichen Schutz von Personendaten lassen sich die folgenden Gründe anführen:

– *Der Datenschutz garantiert keine gerechte Verteilung des Datennutzens*. Zwischen den betroffenen Personen und den Datenbearbeitern herrscht in aller Regel ein Kräfte- und Informationsungleichgewicht.[45] Dieses Ungleichgewicht äussert sich typischerweise darin, dass den betroffenen Personen in Allgemeinen Geschäftsbestimmungen (AGB) weit reichende Einwilligungen abgenommen werden. Ob dies im Rahmen von AGB überhaupt zulässig ist, ist gerichtlich noch nicht geklärt worden.[46] Auch wenn sich in jüngerer Vergangenheit allgemeiner Widerstand gegen einseitige Anpassungen der Datenschutzrichtlinien grosser Unternehmen formiert hat, sind die konkret betroffenen Personen selten bereit, sich gegen allgemeine Bedingungen der mächtigen Gegenseite zur Wehr zu setzen.[47] Zudem sind die Kunden bei der Einwilligung typischerweise auch nicht zu einer angemessenen Folgenabschätzung der Datenbearbeitung in der Lage.
– *Datenschutzrechtliche Ansprüche werden nicht durchgesetzt*. Vielfach ist den betroffenen Personen gar nicht bekannt, dass ihre Daten bearbeitet werden, was die Durchsetzung datenschutzrechtlicher Ansprüche von vornherein verunmöglicht. Eine allgemeine Informationspflicht der Datenbearbeiter besteht nicht; Art. 14 DSG betrifft nur «besonders schützenswerte Personendaten und Persönlichkeitsprofile» und enthält Einschränkungen. Damit wird das Ziel der Transparenz nicht erreicht.[48]
– *Der Schutzgegenstand entspricht nicht dem Schutzbedürfnis der Betroffenen*. Datenschutz schützt keine Daten. Geschützt werden sollen primär die Menschen und ihre Persönlichkeitsrechte.[49] Die Menschen verhalten sich aber oft nicht so, als würde ihnen die vom DSG geschützte Privatsphäre viel bedeuten. Viele Personen geben scheinbar unreflektiert Informationen preis und verwenden keine technischen Hilfsmittel, um ihre Privatsphäre zu schützen,[50] obwohl Umfragen zeigen, dass ihr Vertrauen in Daten sammelnde Systeme und Unternehmen sehr gering ist.[51] Diese Tatsache

---

41 Härting (FN 7), 627.
42 Mayer-Schönberger/Cukier (FN 4), 29; Florent Thouvenin, Grundprinzipien des Datenschutzrechts auf dem Prüfstand, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 61 ff., 67.
43 Thouvenin (FN 42), 68; weniger pessimistisch Epiney (FN 29), N 25, die aufgrund des Prinzips *ad impossibilia nemo tenetur* keinen Verstoss gegen datenschutzrechtliche Vorgaben erkennen will.
44 Thouvenin (FN 42), 66 f.
45 Paul M. Schwartz, Property, Privacy and Personal Data, 117 Harvard Law Review 2004, 2055 ff., 2080 f.; Weber/Oertly (FN 18), N 31.
46 Rolf H. Weber, Big Data: Rechtliche Perspektive, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 17 ff., 25.
47 Schwartz (FN 45), 2081, mit Hinweisen auf das Phänomen der *bounded rationality*.
48 SHK DSG-Wermelinger (FN 13), Art. 14 N 2.
49 SHK DSG-Fey (FN 13), Art. 1 N 2.
50 Mary Madden/Lee Rainie, Americans' Attitudes About Privacy, Security and Surveillance, Pew Research Center, 20.5.2015, Internet: http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (Abruf 4.12.2016), 8 f.
51 Madden/Rainie (FN 50), 7. Neun von zehn US-Amerikanern sind beispielsweise der Ansicht, sie hätten die Kontrolle über ihre Daten verloren, siehe Pew Research Center, Public Perceptions of Privacy and Security in the Post-Snowden Era, Report, 12.11.2014, 3, Internet: http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (Abruf 4.12.2016).

wird in den Geistes- und Sozialwissenschaften mittlerweile mit dem Begriff des *privacy paradox* bezeichnet. Dieses widersprüchliche Verhalten lässt sich möglicherweise verhaltensökonomisch begründen, mag aber auch illustrieren, dass sich die Menschen selbst nicht über ihr Schutzbedürfnis im Klaren sind. Jedenfalls scheint es, als würden spezifische Schutzbedürfnisse nicht durch das Datenschutzrecht abgedeckt.

III. Lösungsansätze

Angesichts der Problemstellung sind zunächst zwei reflexartige Reaktionen naheliegend: Entweder wird das gesamte System des Datenschutzes in Frage gestellt,[52] oder das Datenschutzrecht und seine Grundsätze werden eisern gegen die Zumutungen der Digitalisierung verteidigt.[53]

Die Lösungsmöglichkeiten sind aber vielfältiger. Zunächst kann in Frage gestellt werden, ob es den «grossen Wurf» überhaupt braucht. Denkbar sind nämlich auch branchenspezifische oder unternehmensspezifische Lösungen sowie kleinere Anpassungen innerhalb der datenschutzrechtlichen Normen:

– Für bestimmte Bereiche können mit *gesetzlichen Sondertatbeständen* Rechtfertigungsgründe geschaffen werden. Dies wird namentlich für den Bereich der (quasi-)autonomen Navigation vorgeschlagen.[54]
– Die Verwendung von *Datenschutz-Managementsystemen* senkt zwar nicht die an die Datenbearbeiter gestellten Anforderungen, macht diese Anforderungen aber in der Form von Prozessabläufen steuer- und planbar.[55] Im besten Fall kann sich so eine Kultur etablieren, in der wirksamer Datenschutz zu einem Reputationslabel für die Unternehmen wird.[56]
– Um die Abgrenzung von Personendaten und Sachdaten vorhersehbarer zu machen, wird vorgeschlagen, dass der Gesetzgeber eine *widerlegbare Vermutung des Personenbezugs* aufstellt oder verpflichtende *Prognosen über den Personenbezug der Daten mittels Risikoanalyse* verlangt.[57]

Ins Blickfeld geraten auch Lösungen ausserhalb des Rechts. Unter dem Stichwort *privacy by design* wird seit einigen Jahren ein technischer Ansatz diskutiert, der datenschutzrechtliche Vorgaben bereits in der Designphase einer Anwendung berücksichtigen will. Die Einhaltung rechtlicher Normen soll also nicht mehr nachträglich geprüft werden, sondern bereits bei der Gestaltung des Produkts oder der Dienstleistung einfliessen.[58] Internationale Organisationen, nationale Behörden und Gesetzgeber auf verschiedenen Stufen setzen grosse Hoffnungen in diesen Ansatz.[59] Er hat in Art. 25 auch Eingang in die neue EU-DSGVO gefunden.[60] Dies entspricht dem generellen Trend, technische Lösungen für rechtliche Probleme zu suchen.[61]

Anerkennt man aber die strukturellen Ursachen der in (II.) beschriebenen Problemstellung, müssen die rechtlichen Vorgaben grundsätzlich überdenkt werden. Die Lösung kann dann nicht bloss darin liegen, sich auf die datenschutzfreundliche oder datenschutzfeindliche Seite zu schlagen. Vielmehr muss durch Differenzierungen nach neuen Lösungswegen gesucht werden. In der Wissenschaft sind diesbezüglich zwei Ansätze zu beobachten, auf die es sich näher einzugehen lohnt. Beide sind Gegenstand laufender Forschungsprojekte am *Center for Information Technology, Society, and Law (ITSL)* an der Universität Zürich.

A. Ausweichbewegungen ins Eigentumsrecht

1. Hintergrund

Ausgehend vom Grundgedanken, dass die betroffene Person die «Hoheit über ihre Daten» verloren hat,[62] wird in

---

52 Christopher Kuner/Fred H. Cate/Christopher Millard/Dan Jerker B. Svantesson/Orla Lynskey, The Data Protection Credibility Crisis, 5 International Data Privacy Law 2015, 161: «[T]he current state of data protection regulation around the world […] is marked by a realization that existing regulatory models are not working effectively, the lack of political will to explore alternatives, and general frustration about how to improve the situation.»

53 Epiney (FN 29), N 30; in diese Richtung auch der satirische Beitrag von Beat Rudin, Gebt dem Auto mehr Daten zum Rechnen!, digma 2016, 44.

54 Haustein (FN 14), 99 f. und 107.

55 Weber/Oertly (FN 18), N 24 ff.

56 Weber/Oertly (FN 18), N 36.

57 Hoffmann/Hornung (FN 26), 195, Fn 51 f.

58 Grundlegend: Ann Cavoukian, Privacy by Design, Strong Privacy Protection – Now, and Well into the Future, Toronto 2011.

59 Vgl. OECD, The OECD Privacy Framework 2013, Internet: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (Abruf 11.01.2017); Federal Trade Commission, Protecting Consumers in an Era of Rapid Change, Recommendations for Businesses and Policymakers, FTC Report März 2012, Internet: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (Abruf 11.01.2017).

60 Siehe dazu kritsch Bert-Jaap Koops/Ronald Leenes, Privacy Regulation Cannot Be Hardcoded, 28 International Review of Law, Computers & Technology 2014, 159 ff.

61 Rossnagel (FN 39), 205 f.; Horn (FN 7).

62 Siehe oben II.B.

der Wissenschaft über ein «Eigentum» an Daten nachgedacht.[63] Dieses «Dateneigentum» – bei dem es sich im Übrigen nicht um ein Eigentumsrecht im Sinne von Art. 641 ff. ZGB handeln muss[64] – soll es den Individuen ermöglichen, die Bearbeitung von Daten durch Dritte zu steuern.[65]

Diese Idee ist nicht neu. In den USA gab es schon in den 1990er-Jahren erste Vorstösse zugunsten eines Dateneigentums. Davon erhoffte man sich insbesondere, der wachsenden Flut an Massenwerbung Herr zu werden.[66] In der Tat würde ein *erga omnes* wirkendes Ausschliesslichkeitsrecht die unerlaubte Verwendung von Daten durch Dritte wohl wirksamer begrenzen als die geltenden datenschutzrechtlichen Behelfe. Andererseits kann durchaus argumentiert werden, dass auch letztere bereits heute nahe an die Befugnisse eines *erga omnes* wirkenden Rechts heranreichen.[67]

Derzeit lässt sich noch nicht sagen, ob und gegebenenfalls in welcher Form ein Dateneigentum eingeführt werden sollte. Vielmehr besteht in Bezug auf Begründung und Wesen noch massgeblicher Forschungsbedarf.

2. Erwartungen

Von einem Dateneigentum erhofft man sich, dass die betroffenen Personen wieder Herr über ihre Daten werden. Insbesondere sollen die *bei der Verwendung von Daten anfallenden Kosten und der gewonnene Nutzen gerechter verteilt werden*. Ein oft gehörtes Argument besagt, Daten sammelnde Unternehmen würden den Nutzen der Daten internalisieren, während sie die Kosten (vor allem die negativen Auswirkungen auf die Privatsphäre) an die betroffenen Personen externalisieren.[68] Für einige Stimmen ist dies das entscheidende Argument für die Einführung eines Dateneigentums.[69] Gleichzeitig werden in der Lehre erhebliche Zweifel gehegt, ob das angestrebte Ziel durch die Einräumung eines *erga omnes* wirkenden Rechts tatsächlich erreicht werden kann. Am Kräfte- und Informationsungleichgewicht zwischen betroffenen Personen und Daten sammelnden Unternehmen ändert sich dadurch nämlich auf den ersten Blick wenig.[70] Befürchtet wird sogar, dass viele Bürger Daten ungebremst preisgeben, während andere dies verweigern und so letztlich eine «Zwei-Klassen-Datengesellschaft» entsteht, in der sich nur Wohlhabendere eine Privatsphäre leisten können.[71] Um diesem Ungleichgewicht entgegenzuwirken, müssen die betroffenen Personen ihre Kräfte (bzw. Daten) aller Voraussicht nach bündeln, wobei sich genossenschaftliche Modelle anbieten. Solche Ideen werden gegenwärtig im Bereich der Gesundheitsdaten getestet.[72]

Von der Einführung eines Dateneigentums erhofft man sich zudem die *Senkung von Transaktionskosten*. Gemeint sind Kosten im Zusammenhang mit dem Entwerfen, Verstehen und Einhalten von Verträgen, AGB und Datenschutzerklärungen. Hinzu kommen aber auch Such- und Verhandlungskosten.[73] Wie hoch diese Transaktionskosten gegenwärtig sind und ob sie nach der Einführung eines Dateneigentums tatsächlich tiefer wären, ist – soweit ersichtlich – bislang nicht mit quantitativen Mitteln erforscht worden.

Weiter bringen die Befürworter eines Dateneigentums vor, eine eindeutige Zuweisung von Daten zu einem Rechtsträger wäre ein klarer Ausgangspunkt für Vertragsverhandlungen und würde damit *Rechtssicherheit* schaf-

---

63 Zum Stand der Diskussion siehe Florent Thouvenin/Alfred Früh/Alexandre Lombard, Eigentum an Sachdaten: Eine Standortbestimmung, SZW 2017, 2 ff., sowie Florent Thouvenin, Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs, SJZ 2017, 21 ff.

64 Denkbar sind mindestens fünf verschiedene Ausformungen dieser Rechtsfigur, vgl. Thouvenin/Früh/Lombard (FN 63), 4 ff. Der Begriff des Dateneigentums wird bloss der Einfachheit halber verwendet und indiziert keine Präferenz zugunsten einer bestimmten Ausformung.

65 Weber (FN 11), N 42.

66 Siehe Kenneth C. Laudon, Markets and Privacy, 39 Communications of the ACM 9/1996, 92 ff., 102.

67 Thouvenin (FN 63), 27.

68 Andreas Wiebe, Protection of Industrial Data – a New Property Right for the Digital Economy?, GRUR Int. 2016, 877 ff., 881; Wolfgang Kilian, Personal Data: The Impact of Emerging Trends, CRi 2012, 169 ff., 172; Matthias Berberich/Sebastian Golla, Zur Konstruktion eines «Dateneigentums» – Herleitung, Schutzrichtung, Abgrenzung, PinG 2016, 165 ff.; Dorner (FN 23), 626 m.w.H. in Fn 118; Schwartz (FN 45), 2079.

69 Siehe Herbert Zech, «Industrie 4.0» – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 ff., 1160, der die Auffassung vertritt, die neue Zuordnung des Nutzens würde eine Transparenzkultur fördern und das Datenerzeugerrecht hätte für «open data» die gleiche Funktion wie das Urheberrecht für «open source»; vgl. weiter den *Propertization*-Ansatz von Schwartz (FN 45), 2094 ff., und Verweise auf den sog. *endowment effect,* wonach Individuen ein Gut höher einschätzen, wenn es ihnen zugeteilt worden ist.

70 Gerrit Hornung/Thilo Goeble, «Data Ownership» im vernetzten Automobil, CR 2015, 265 ff., 268; Thilo Weichert, Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, 1463 ff., 1468 f.; Niko Härting, «Dateneigentum» – Schutz durch Immaterialgüterrecht, CR 2016, 646 ff., 649; grundlegend auch Benedikt Buchner, Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006, 103 ff.; Jessica Litman, Information Privacy/Information Property, 52 Stanford Law Review 2000, 1283 ff.

71 Härting (FN 70), 648.

72 Vgl. die Initiativen healthbank.coop und MIDATA.coop.

73 Siehe Joshua A. T. Fairfield, Virtual Property, 85 Boston University Law Review 2005, 1047 ff., 1090.

fen.[74] Die Zuordnung des Schutzgegenstandes zu einem Rechtsträger erweist sich aber als schwierig (siehe sogleich III.A.3.) und eine Rechtsunsicherheit im eigentlichen Sinne existiert gegenwärtig nicht.[75]

3. Schwierigkeiten

Die Zuweisung neuer Ausschliesslichkeitsrechte an Einzelne bedeutet zugleich eine Einschränkung der Allgemeinheit und damit eine neue Güterzuordnung. Die Einführung eines Eigentumsrechts an Daten ist also *rechtfertigungsbedürftig*.[76] Dieser Tatsache wird oft zu wenig Aufmerksamkeit geschenkt.[77] Eine Analyse der für ein Dateneigentum vorgebrachten Rechtfertigungsgründe zeigt, dass diese *prima vista* wenig überzeugend sind.[78] Mit Blick auf das berechtigte Anliegen, Kosten und Nutzen der Datenbearbeitung gerechter zu verteilen, besteht aber nach wie vor Forschungsbedarf.

Unklar ist gegenwärtig auch noch, was der *Gegenstand eines Dateneigentums* wäre. Die intuitive Antwort «Daten» ist zwar sicher richtig, aber wohl zu wenig bestimmt.[79] Insbesondere scheint noch unklar zu sein, ob der Schutz an der (syntaktischen) Ebene des Datums als Zeichen oder an der (semantischen) Ebene der sinnhaften Information ansetzen soll.[80] Die Entscheidung hat weit reichende Konsequenzen für den Schutzbereich des Dateneigentums.

Ebenso unklar ist, wer *originärer Rechtsinhaber* sein soll.[81] Die Lehre unterscheidet hier bislang noch zwischen Personendaten und Sachdaten, obwohl diese Differenzierung gerade im Kontext eines potenziellen Dateneigentums zu überdenken wäre. Bezüglich Sachdaten wurde bisher das Ansetzen am Skripturakt, das heisst am Vorgang der Erzeugung oder Speicherung von Daten, vorgeschlagen. Massgebend soll sein, wer die Skriptur wesentlich beeinflussen kann[82] oder wer der wirtschaftliche Betreiber[83] des Systems ist. Auch diese Begriffe erlauben aber noch keine eindeutige Zuordnung;[84] möglicherweise sind die Interessenkonstellationen im Einzelfall sogar zu vielfältig, um ein einheitliches Zuordnungskriterium zu finden.[85] Bei personenbezogenen Daten wirft die Zuordnung der Inhaberschaft weniger Probleme auf. Inhaberin oder Inhaber ist die betroffene Person selbst. Einzig bei genetischen Daten, die nicht nur die betroffene Person selbst, sondern auch deren Verwandte betreffen, wird die Zuordnung komplizierter.[86]

Eine Schlüsselfrage im Zusammenhang mit einem potenziellen Dateneigentum ist jene nach der *Rolle des Datenschutzrechts*. Die Probleme des zu weit reichenden Datenschutzrechts lassen sich nur lösen, wenn zumindest Teile davon vom Dateneigentum ersetzt würden. Andernfalls würde lediglich eine zusätzliche Ebene von Rechten eingefügt. Der unter (II.B.) thematisierte zu wenig weit reichende Schutz würde zwar möglicherweise erweitert, ohne aber die in (II.A.) aufgeführten Folgen des zu weit reichenden Datenschutzes zu verhindern. In der Lehre scheint die Meinung vorzuherrschen, das Datenschutzrecht hätte nach der Einführung eines Dateneigentums noch seine Berechtigung, wenngleich in reduziertem Umfang.[87]

---

74 Herbert Zech, Daten als Wirtschaftsgut – Überlegungen zu einem «Recht des Datenerzeugers», CR 2015, 137 ff., 145.

75 Siehe hierzu Thouvenin/Früh/Lombard (FN 63), 8 f.

76 Thouvenin/Früh/Lombard (FN 63), 7.

77 Oft wird ganz auf eine Begründung oder Rechtfertigung verzichtet, siehe z.B. Urs Hess-Odoni, Die Herrschaftsrechte an Daten, Jusletter vom 17.5.2004, Einleitung und N 20, oder die Autoren begnügen sich mit der Feststellung, Daten seien werthaltig und nur schon deswegen durch ein Dateneigentum zu schützen, siehe Robert G. Briner, Big Data und Sachenrecht, Jusletter IT vom 21.5.2015; Thomas Hoeren, Big Data and the Ownership in Data: Recent Developments in Europe, EIPR 2014, 751 ff., 753; Martin Eckert, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 2016, 245 ff., 246.

78 Ausführlich Thouvenin/Früh/Lombard (FN 63), 7 ff.

79 Josef Drexl et al., Positionspapier des Max-Planck-Instituts für Innovation und Wettbewerb, 16.8.2016, N 8; Wiebe (FN 68), 883 f., nennt dies das Spezifizierungsproblem.

80 Daniel Hürlimann/Herbert Zech, Rechte an Daten, sui-generis 2016, 89 ff., 94; in der Tendenz für einen Schutz auf der syntaktischen Ebene Wolfgang Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRUR Int. 2016, 989 ff., 992; Louisa Specht, Ausschliesslichkeitsrechte an Daten, CR 2016, 288 ff., 290; Eckert (FN 77), 247; Zech (FN 74), 138 f.; tendenziell für einen Schutz auf der semantischen Ebene Hess-Odoni (FN 77), N 6.

81 Heymann (FN 23), 654 f.; Wiebe (FN 68), 883 f., nennt dies das Zuordnungsproblem.

82 Thomas Hoeren, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 ff., 488.

83 Zech (FN 69), 1159; Zech (FN 74), 144.

84 Siehe auch Jan Christian Sahl, Gesetz oder kein Gesetz, das ist hier die Frage, PinG 2016, 146 ff., 149.

85 Heymann (FN 23), 655.

86 Nadezhda Purtova, The Illusion of Personal Data as No One's Property, 7 Law Information and Technology, 2015, 83 ff., 110.

87 Zum Zusammenspiel von Dateneigentum und Datenschutzrecht siehe Thouvenin (FN 63), 30 f.; vom Datenschutzrecht als einer notwendigen Schranke eines künftigen Dateneigentums sprechen Berberich/Golla (FN 68), 166 f.; Zech (FN 69), 1160, spricht von einem Nebeneinander der verschiedenen Zuweisungsordnungen.

B. Neukonzeption von Privacy

1. Hintergrund

Die Problemstellung deutet darauf hin, dass zwischen Privacy als gesellschaftlichem Konstrukt einerseits und dem Datenschutz andererseits ein Missverhältnis besteht.[88] Dass das Datenschutzrecht einerseits zu viel und andererseits zu wenig schützt, indiziert, dass man gründlicher über dessen Schutzgegenstand nachdenken sollte.[89] Gefordert wird deshalb zu Recht, den Datenschutz dem heute vorherrschenden Verständnis von Privacy anzugleichen.[90] Das wirft die zentrale Frage auf, was unter Privacy überhaupt verstanden wird.

2. Erwartungen

Bisher gibt es keine kohärente interdisziplinäre Forschung, die sich damit auseinandersetzt, was Privacy bedeutet. Weil Privacy aber keine normative Konstante ist,[91] sondern das Bedürfnis nach Privacy gesellschaftlichen Strömungen unterworfen ist, braucht es Antworten aus mehreren Disziplinen, um ein besseres Verständnis des Schutzgegenstandes zu gewinnen. Zu berücksichtigen ist beispielsweise, dass auch die technologische Entwicklung den Gehalt von Privacy verändert. Zudem können verschiedene Nutzergruppen innerhalb der gleichen Gesellschaft unterschiedliche Privacy-Bedürfnisse haben.[92]

Auf der Grundlage eines allgemeinen Verständnisses von Privacy könnten die betroffenen Personen angemessen geschützt werden, womöglich ohne das immense Potential der Nutzung von Personendaten über Gebühr zu beeinträchtigen. Prognosen über die Richtung dieses Schutzes sind noch verfrüht. Anstelle des herkömmlichen Sphärenmodells des Persönlichkeitsschutzes werden bestimmt andere Konzepte im Vordergrund stehen. Es lässt sich mutmassen, dass es unter anderem um die freie Kontextualisierung persönlicher Information geht; die betroffene Person soll selbst darüber entscheiden können, innerhalb welcher Kontexte welche ihrer persönlichen Informationen verwendet werden dürfen. Gleichzeitig würde der jeweilige Kontext der Nutzung persönlicher Informationen Grenzen setzen.

3. Schwierigkeiten

Gegen eine Neukonzeption von Privacy mag man einwenden, der Zeitpunkt sei denkbar ungünstig: Soeben wurde die EU-DSGVO verabschiedet und auch die Schweizer Revision des DSG dürfte keinen grundsätzlichen Systemwechsel mit sich bringen.

Der Weg zu einem neuen oder zeitgemässen Verständnis des Schutzgegenstands Privacy ist in jedem Fall noch lang und steinig, nicht zuletzt weil er koordinierte interdisziplinäre Anstrengungen erfordert. Wird dieser Pfad in der Forschung indes konsequent eingeschlagen, stehen spätestens bei der nächsten Revision des Datenschutzrechts die dringend benötigten neuen Ansätze bereit.

IV. Fazit

Datenbasierte Systeme können in den unterschiedlichsten Bereichen eingesetzt werden. Typische Beispiele sind das selbstfahrende Automobil, der sich selbst füllende Kühlschrank, der Diagnoseroboter oder der Pflegeroboter. Gemeinsam ist ihnen die Funktionsweise: Sie nehmen in komplexen Umweltsituationen mittels Sensoren Daten auf, passen – oft mittels Rückgriff auf umfangreiche Datenbestände – selbständig Programmabläufe an und handeln damit zunehmend autonom.

Aus informationsrechtlicher Sicht stellen diese datenbasierten Systeme die Rechtsordnung vor erhebliche Probleme. Insbesondere der Anwendungs- und und Wirkungsbereich des Datenschutzrechts reicht so weit, dass viele neue Anwendungen gefährdet sind. Dies lässt sich auf die technische Entwicklung und die Tatsache zurückführen, dass das Datenschutzrecht auf prä-digitalen Konzepten basiert. Gleichzeitig lässt sich aber feststellen, dass das Datenschutzrecht die Privatsphäre der betroffenen Personen trotz der Ausdehnung seines Anwendungsbereichs nicht adäquat schützt. Es bestehen damit Indizien für eine grundlegende Diskrepanz zwischen dem Schutzgegenstand und den Schutzwirkungen des Datenschutzrechts.

Zwar kann das (insoweit dysfunktionale) System mit spezifischen Normen punktuell verbessert werden. Die strukturellen Probleme lassen sich allerdings nur lösen, wenn Schutzgegenstand und Schutzwirkungen des Datenschutzrechts wieder in Übereinstimmung gebracht werden. In der Wissenschaft werden gegenwärtig zwei Ansätze näher untersucht, denen dies zugetraut wird: das

---

88 Siehe oben II.; Brunner (FN 37), 9.

89 Siehe bereits Patricia Mell, Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness, 11 Berkeley Technology Law Journal 1996, 1 ff., 3.

90 Brunner (FN 37), 9.

91 Zur Vielschichtigkeit des Begriffs: Daniel J. Solove, A Taxonomy of Privacy, 154 University of Pennsylvania Law Review 2006, 477 ff.

92 Brunner (FN 37), 9.

Konzept eines Dateneigentums sowie eine Neukonzeption des Schutzgegenstands Privacy.

Vom *Dateneigentum* erhofft man sich, dass die betroffenen Personen die Herrschaft über ihre Daten zurückerlangen. Ziele sind ausserdem die Reduktion von Transaktionskosten und mehr Rechtssicherheit. Erste Ergebnisse zeigen, dass vieles noch offen ist, der Erfolg aber unter anderem davon abhängt, ob das Dateneigentum gewisse datenschutzrechtliche Funktionen übernehmen kann, die gegenwärtig zu weit reichen. Zugleich muss sich das Kräfte- und Informationsgleichgewicht zwischen Unternehmen und der betroffenen Person zugunsten Letzterer verschieben. Das Dateneigentum allein reicht dafür allerdings kaum aus.

Ein zweiter Ansatz fokussiert auf den *Schutzgegenstand Privacy*. Nur wenn klar ist, was das Gesetz schützen will, kann es auch angemessen ausgestaltet werden. Privacy ist aber keine normative Konstante, sondern gesellschaftlichen Veränderungen unterworfen. Deswegen muss die Frage nach dem Schutzgegenstand interdisziplinär und sehr grundsätzlich angegangen werden. Die Forschung hierzu steht noch ganz am Anfang.